PENETRAČNÍ TESTOVÁNÍ

Technická *zpráva.*

DontBeHacked s. r. o. — účetní a mzdový systém. Detailní technické nálezy, reprodukční kroky a doporučení k opravě.

KLIENT	OBDOBÍ	NÁLEZY	DATUM ZPRÁVY
DontBeHacked s. r. o.	1. – 7. 4. 2026	● 1 ● 2 ● 2 ● 2	8. dubna 2026

OBSAH

Struktura *dokumentu.*

URČENÍ DOKUMENTU · DISTRIBUCE

Tento dokument je určen **výhradně pro technický tým klienta** odpovědný za opravu identifikovaných zranitelností. Obsahuje reprodukční kroky, zdrojový kód, konfigurace a další technické detaily, jejichž zneužití by neoprávněné osobě umožnilo kompromitaci systému. **Nekopírujte a nesdílejte tento dokument mimo dohodnutý okruh příjemců.**

Paralelně byla klientovi doručena **Zpráva pro vedení** — netechnický souhrn nálezů, byznys dopadu a doporučených priorit. Je určena pro management a neobsahuje reprodukční detaily.

Testovaná *aktiva.*

AKTIVUM	TYP	VERZE / BUILD
`app.dontbehacked.sk`	Webová aplikace (React 18 + ASP.NET Core 6)	Build 4.2.1-rc3
`api.dontbehacked.sk`	REST API (.NET 6, Swagger / OpenAPI 3.0)	v2.8.0
`sk.dontbehacked.app`	Android APK (Kotlin, minSdk 26)	v4.2.1 (versionCode 89)
`admin.dontbehacked.sk`	Administrátorský portál (React + ASP.NET)	Build 2.1.4
`*.dontbehacked.sk`	Subdomény (38 identifikovaných, 22 live)	—

Metodologie

Externí penetrační testování dle OWASP Testing Guide v4.2, PTES (Penetration Testing Execution Standard) a NIST SP 800-115. Tři fáze: (1) automatizované skenování povrchu a závislostí, (2) statická analýza dekompilovaného kódu, (3) manuální testování a verifikace nálezů. AI-podpořený výzkum zrychluje první fázi; každý nález prochází expertní validací před zápisem do zprávy. Všechny testy probíhaly z externího prostředí přes komerční VPN; žádné testy z interní sítě klienta.

Omezení

Testování nepokrývá interní síť, fyzickou bezpečnost, sociální inženýrství ani systémy třetích stran (Azure control plane, platební bránu, CDN). Destruktivní testování a hromadná extrakce dat nebyly prováděny — tam, kde je exploit destruktivní, je to výslovně uvedeno a závažnost upravena v souladu s pravidlem ***„demonstrace omezená rozsahem“***.

Klasifikace závažnosti

ÚROVEŇ	DEFINICE	TERMÍN OPRAVY
KRITICKÝ	Existenční ohrožení — masivní únik dat, plná kompromitace infrastruktury, supply chain	Okamžitě (do 48 h)
VYSOKÝ	Vážná škoda — omezený únik dat, kompromitace administrátora, obejití autentizace	Do 7 dnů

	potenciál zneužití insiderem	Nejbližší release
INFO	Hygienické pozorování — chybějící hlavičky, rozšířené chyby, zastaralé knihovny bez exploitu	Maintenance cyklus

Architektura DontBeHacked z pohledu *útočníka.*

Během rekognoskace jsme identifikovali následující externí infrastrukturu:

KOMPONENTA	TECHNOLOGIE	POZNÁMKA
Frontend	React 18 za Cloudflare CDN	SPA, bez SSR
API backend	ASP.NET Core 6, Kestrel za nginx reverse proxy	Swagger UI přístupný na `/swagger`
Databáze	PostgreSQL 14 (inferováno z Npgsql v stack trace)	Externě nepřístupná
Úložiště	Azure Blob Storage (`dontbehackedprod`)	Klíč v APK — viz F-03
Mobilní aplikace	Kotlin, OkHttp 4.12, cert pinning chybí	Distribuce přes Google Play
Admin portál	React + ASP.NET, stejný API backend	Externě přístupný — viz F-04
E-mail	SMTP přes SendGrid (API key v app config)	Transakční zprávy
Autentizace	JWT RS256, refresh tokeny, bez MFA	Rate limiting chybí — viz F-05

Identifikované subdomény

Z 38 identifikovaných subdomén (`crt.sh` + `subfinder`) bylo 22 živých. Kromě primárních aktiv (viz sekce 01) jsme identifikovali:

SUBDOMÉNA	STAV	POZNÁMKA
`staging.dontbehacked.sk`	200 OK	Staging s produkční databází (stejná data jako prod)
`grafana.dontbehacked.sk`	302 → login	Grafana 10.2.1, výchozí admin login netestován
`jenkins.dontbehacked.sk`	403	Jenkins za IP whitelistem

`docs.dontbehacked.sk`	200 OK	Interní API dokumentace, veřejně přístupná
`legacy-api.dontbehacked.sk`	200 OK	Starší API verze (v1), stále aktivní, stejná databáze
`mail.dontbehacked.sk`	443 timeout	MX záznam, SMTP

Pozoruhodné: `staging.dontbehacked.sk` sdílí produkční databázi. Všechny API nálezy (F-01, F-02, F-05) jsou reprodukovatelné i na staging endpointu. Staging nemá Cloudflare ochranu, což snižuje bariéru pro útočníka.

IDOR — neoprávněný přístup k mzdovým *datům.*

F-01 KRITICKÝ **Broken Access Control na payroll API endpointech**

CWE	OWASP	AKTIVUM	OVĚŘENÍ
CWE-862	A01:2021	`api.dontbehacked.sk`	Reprodukováno (live)

POPIS ZRANITELNOSTI

Endpoint `/api/v2/payroll/employees/{companyId}` přijímá parametr `companyId` přímo z URL path, ale **neověřuje, zda přihlášený uživatel patří k požadované společnosti**. Parametr je sekvenční celé číslo v rozsahu 1 – ~ 4 200. Útočník s běžným trial účtem (registrace trvá 30 sekund) získá přístup k mzdovým záznamům libovolné společnosti v systému.

Stejný vzorec chybějící autorizace jsme identifikovali na dalších **14 endpointech** v `/api/v2/payroll/*` namespace včetně `/payslips`, `/tax-returns`, `/social-insurance` a `/bank-accounts`.

REPRODUKČNÍ KROKY

1. Registrace trial účtu na `app.dontbehacked.sk/register` (e-mail + heslo)
2. Přihlášení přes `POST /api/v2/auth/login` → Bearer JWT token
3. Odeslání požadavku s cizím `companyId`:

```
GET /api/v2/payroll/employees/12345 HTTP/1.1
Host: api.dontbehacked.sk
Authorization: Bearer eyJhbGciOiJSUzI1NiIs...zkráceno
Accept: application/json
```

ODPOVĚĎ SERVERU (REDIGOVANÁ PII)

```
HTTP/1.1 200 OK
Content-Type: application/json
X-Request-Id: 7f3a2b1c-4d5e-6f7a-8b9c-0d1e2f3a4b5c

{
  "companyId": 12345,
  "companyName": "[redacted] s.r.o.",
  "ico": "[redacted]",
  "employees": [
    {
      "employeeId": 89234,
      "firstName": "[redacted]",
      "lastName": "[redacted]",
      "birthNumber": "[redacted]/[redacted]",
      "personalIdNumber": "[redacted]",
      "bankAccount": "SK[redacted]",
      "address": "[redacted], [redacted]",
      "grossSalary": [redacted],
      "netSalary": [redacted],
      "taxBase": [redacted],
      "healthInsurance": [redacted],
      "socialInsurance": [redacted]
    }
    // ... další zaměstnanci
  ],
  "totalEmployees": 47,
  "generatedAt": "2026-04-08T14:22:31Z"
}
```

DŮKAZ

Ověřeno na 3 náhodných `companyId` hodnotách (12345, 12346, 12400). Každá vrátila kompletní mzdové záznamy jiné společnosti. Extrahovány jen první dva záznamy z každé odpovědi — hromadná extrakce nebyla provedena.

SHA-256 odpovědi (companyId=12345):
`e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855`

Dotčené endpointy (stejný vzorec): `/api/v2/payroll/employees/{id}`, `/payslips/{id}`, `/tax-returns/{id}`, `/social-insurance/{id}`, `/bank-accounts/{id}`, `/attendance/{id}`, `/contracts/{id}`, `/bonuses/{id}`, `/deductions/{id}`, `/departments/{id}`, `/positions/{id}`, `/salary-history/{id}`, `/documents/{id}`, `/exports/{id}`, `/reports/{id}`.

DOPAD

Při ~ 4 200 aktivních společnostech a průměrně ~ 20 zaměstnancích na společnost je exponováno **~ 85 000 kompletních mzdových záznamů** včetně: jméno, rodné číslo, číslo OP, adresa, bankovní účet, výše platu, daňové podklady, zdravotní a sociální odvody, pracovní smlouvy.

Údaje spadají pod GDPR čl. 9 (zvláštní kategorie) a slovenský zákon č. 18/2018 Z. z. Slovenský ÚOOÚ je oprávněn uložit sankci až do výše **4 % ročního obratu**.

DOPORUČENÍ K OPRAVĚ

Implementovat autorizační kontrolu na úrovni middleware nebo controlleru. Každý požadavek musí ověřit, že `companyId` odpovídá společnosti přiřazené autentizovanému uživateli:

```
// PayrollController.cs — přidat na všech 15 endpointech
[Authorize]
public async Task<IActionResult> GetEmployees(int companyId)
{
    var userCompanyId = User.Claims
        .First(c => c.Type == "company_id").Value;
    if (companyId.ToString() != userCompanyId)
        return Forbid();

    // ... původní logika
}
```

Alternativa (dlouhodobě lepší): globální authorization filter na úrovni `/api/v2/payroll/*` route group, který automaticky extrahuje `companyId` z pathu a porovná s claimem v JWT. Eliminuje riziko zapomenuté kontroly na novém endpointu.

Vzdálené spuštění kódu přes *deserializaci.*

F-02 VYSOKÝ **RCE přes Newtonsoft.Json TypeNameHandling.Auto**

CWE	ADVISORY	AKTIVUM	OVĚŘENÍ
CWE-502	GHSA-5crp-9r3c-p9vr	`api.dontbehacked.sk`	Statická analýza

POPIS

Dekompilovaný kód API serveru (ilspycmd → C#) obsahuje globální konfiguraci JSON deserializace s nastavením `TypeNameHandling.Auto` v knihovně Newtonsoft.Json 12.0.3. Toto nastavení útočníkovi umožňuje vložit do těla JSON požadavku referenci na libovolný .NET typ — včetně typů jako `System.Diagnostics.Process`, `System.IO.File` a gadget chainů pro vzdálené spuštění kódu.

```
// DontBeHacked.Api.Startup.cs (decompiled, line 147)
services.AddControllers()
    .AddNewtonsoftJson(options =>
    {
        options.SerializerSettings.TypeNameHandling =
            TypeNameHandling.Auto;  // ← zranitelné nastavení
        options.SerializerSettings.NullValueHandling =
            NullValueHandling.Ignore;
    });
```

SCÉNÁŘ ZNEUŽITÍ

Útočník identifikuje API endpoint, který přijímá polymorfní JSON objekt (např. `POST /api/v2/payroll/import` s obecným parametrem `object`) a odešle payload obsahující gadget chain:

```
{
  "$type": "System.Windows.Data.ObjectDataProvider, PresentationFramework",
  "MethodName": "Start",
  "MethodParameters": {
    "$type": "System.Collections.ArrayList",
    "$values": ["cmd", "/c calc.exe"]
  },
  "ObjectInstance": {
    "$type": "System.Diagnostics.Process, System"
  }
}
```

Demonstrace omezená rozsahem testování — odeslání exploit payloadu by způsobilo spuštění kódu na produkčním serveru. Zranitelnost je potvrzena statickou analýzou kódu a přesnou shodou verze knihovny s publikovaným advisory.

DOPAD

Vzdálené spuštění libovolného kódu na aplikačním serveru v kontextu servisního účtu. Dále: přístup k PostgreSQL databázi (connection string v `appsettings.json`), klíčům k Azure Storage, API klíči SendGrid a síťovým zdrojům dostupným z aplikačního serveru.

DOPORUČENÍ K OPRAVĚ

Změnit globální nastavení na bezpečnou hodnotu:

```
options.SerializerSettings.TypeNameHandling =
    TypeNameHandling.None;  // bezpečné — výchozí hodnota
```

Pokud je polymorfní deserializace nutná pro konkrétní endpointy (např. import), implementovat vlastní `ISerializationBinder` s explicitním whitelistem povolených typů. Nikdy nepoužívat `Auto` nebo `All` na endpointech přijímajících externí vstup.

Zvážit migraci z Newtonsoft.Json na `System.Text.Json` (nativní .NET), který nemá ekvivalent `TypeNameHandling` a je bezpečný ve výchozím nastavení.

Hardcoded Azure Storage *master key.*

F-03 VYSOKÝ **Azure Storage Account key v plaintextu v mobilní aplikaci**

CWE	OWASP	AKTIVUM	OVĚŘENÍ
CWE-798	A07:2021	`sk.dontbehacked.app`	Reprodukováno (read-only)

POPIS

Dekompilovaný kód mobilní aplikace (jadx) obsahuje přístupový klíč k Azure Blob Storage v plaintextové konstantě. Klíč je **master key** — poskytuje plný přístup (čtení, zápis, mazání) ke všem kontejnerům v storage účtu.

```
// sk/dontbehacked/app/config/CloudConfig.java (jadx output)
public static final String STORAGE_ACCOUNT = "dontbehackedprod";
public static final String STORAGE_KEY =
    "[redacted]";
public static final String CONTAINER = "customer-exports";
```

REPRODUKČNÍ KROKY

1. Stáhnout APK z Google Play nebo APKPure
2. Dekompilovat: `jadx -d output/ sk.dontbehacked.app.apk`
3. Najít klíč: `grep -r "STORAGE_KEY" output/`
4. Ověřit přístup (read-only, žádná data nestažena):

```
$ az storage container list \
    --account-name dontbehackedprod \
    --account-key "[redacted]" \
    --output table

Name               Lease Status    Last Modified
-----------------  --------------  -------------------------
customer-exports   unlocked        2026-04-07T09:14:22+00:00
payroll-backups    unlocked        2026-04-06T02:00:15+00:00
documents          unlocked        2026-04-08T11:33:47+00:00
temp-imports       unlocked        2026-04-08T14:22:01+00:00
```

> **DŮKAZ**
>
> Klíč ověřen přes `az storage container list` — vráceny 4 kontejnery. Kontejner `payroll-backups` podle názvu obsahuje zálohy mzdových dat. Žádná data nebyla stažena ani modifikována.

DOPAD

Kdokoliv s přístupem k APK (veřejně dostupné na Google Play) může extrahovat klíč a získat plný přístup k storage účtu včetně potenciálních záloh databáze a zákaznických exportů. Klíč je sdílen napříč všemi instalacemi aplikace.

> **DOPORUČENÍ K OPRAVĚ**
>
> 1. **Okamžitě:** rotovat oba klíče účtu `dontbehackedprod` (primární + sekundární).
> 2. **Okamžitě:** zkontrolovat Azure Storage Analytics log za posledních 90 dní pro nestandardní přístupy.
> 3. **Krátkodobě:** nahradit hardcoded klíč server-generovanými SAS tokeny s omezeným scope a platností (max. 1 hodina).
> 4. **Dlouhodobě:** implementovat Azure Managed Identity nebo Azure AD RBAC — eliminuje statické klíče úplně.

Admin rozhraní přístupné z *internetu.*

F-04 STŘEDNÍ **Administrátorský portál bez síťového omezení**

CWE	OWASP	AKTIVUM	OVĚŘENÍ
CWE-749	A05:2021	`admin.dontbehacked.sk`	Potvrzeno

POPIS

Administrátorský portál na `admin.dontbehacked.sk` je dostupný z libovolné IP adresy bez VPN, IP whitelistu nebo jiného síťového omezení. Přihlašovací formulář je veřejně přístupný. V kombinaci s nálezem F-05 (chybějící rate limiting) útočník může automatizovaně zkoušet hesla admin účtů.

DOPAD

Úspěšné přihlášení by poskytlo přístup ke správě zákazníků, licencí, systémových nastavení a uživatelských účtů. Admin portál používá stejný API backend — admin JWT token má scope `admin:*` oproti běžnému `user:read`.

DOPORUČENÍ K OPRAVĚ

Omezit přístup k `admin.dontbehacked.sk` na firemní VPN nebo definovaný rozsah IP adres na úrovni nginx / Cloudflare Access. Jako alternativu implementovat mTLS s klientským certifikátem. Doplnit vícefaktorovou autentizaci (TOTP nebo WebAuthn) na admin login.

Chybějící rate limiting na *přihlášení.*

F-05 STŘEDNÍ **Neomezený počet pokusů o přihlášení**

CWE	OWASP	AKTIVUM	OVĚŘENÍ
CWE-307	A07:2021	`api.dontbehacked.sk`	Reprodukováno

POPIS

Endpoint `POST /api/v2/auth/login` neimplementuje žádný mechanismus omezení rychlosti ani počtu neúspěšných pokusů. Odeslání 50 nesprávných hesel z jedné IP adresy za 10 sekund nevyvolalo žádné blokování, CAPTCHA ani zpoždění odpovědi.

```
# 50 pokusů, průměrná odezva 84 ms, žádná 429
$ for i in $(seq 1 50); do
    curl -s -o /dev/null -w "%{http_code} %{time_total}s\n" \
      -X POST https://api.dontbehacked.sk/api/v2/auth/login \
      -H "Content-Type: application/json" \
      -d "{\"email\":\"admin@dontbehacked.sk\",\"password\":\"guess$i\"}"
  done | head -5

401 0.084s
401 0.079s
401 0.091s
401 0.082s
401 0.088s
... (všech 50 stejně, žádná 429)
```

DOPORUČENÍ K OPRAVĚ

Implementovat rate limiting na `/api/v2/auth/login` : max. 5 neúspěšných pokusů za 15 minut na kombinaci IP + e-mail. Po třetím neúspěšném pokusu zobrazit CAPTCHA. Po desátém pokusu dočasně zablokovat účet (30 min). Vracet `429 Too Many Requests` s hlavičkou `Retry-After` .

Zastaralé *závislosti.*

F-06 INFO **Knihovny s publikovanými bezpečnostními advisory**

CWE	OWASP	AKTIVUM	OVĚŘENÍ
CWE-1104	A06:2021	`api.dontbehacked.sk`	Statická analýza

POPIS

Statická analýza (`osv-scanner` na dekompilovaných assembly referencích) identifikovala čtyři knihovny s vydanými bezpečnostními opravami. Pro žádnou z nich jsme neidentifikovali přímo zneužitelnou cestu v kontextu DontBeHacked — zařazeny jako informativní pozorování.

KNIHOVNA	NALEZENÁ VERZE	OPRAVENÁ VERZE	ADVISORY
`System.Text.Json`	6.0.0	8.0.5+	GHSA-hh2w-p6rv-4g7w
`BouncyCastle`	1.8.9	2.4.0+	CVE-2024-29857
`Npgsql`	6.0.4	8.0.6+	CVE-2024-32655
`jQuery`	3.5.1	3.7.1+	CVE-2020-23064

DOPORUČENÍ

Aktualizovat na opravené verze v rámci nejbližšího maintenance cyklu. Zavést automatické skenování závislostí (např. `dotnet list package --vulnerable` v CI pipeline, Dependabot nebo Renovate pro mobilní a webové projekty).

Chybějící HTTP bezpečnostní *hlavičky.*

F-07 INFO **Webový portál neodesílá doporučené security headers**

CWE	OWASP	AKTIVUM	OVĚŘENÍ
CWE-693	A05:2021	`app.dontbehacked.sk`	Potvrzeno

POPIS

Odpovědi z `app.dontbehacked.sk` neobsahují následující bezpečnostní hlavičky doporučené OWASP Secure Headers Project:

HLAVIČKA	STAV	DOPORUČENÁ HODNOTA
`Content-Security-Policy`	Chybí	`default-src 'self'; script-src 'self'; style-src 'self' 'unsafe-inline'`
`Strict-Transport-Security`	Chybí	`max-age=31536000; includeSubDomains; preload`
`X-Content-Type-Options`	Chybí	`nosniff`
`Permissions-Policy`	Chybí	`camera=(), microphone=(), geolocation=()`
`Referrer-Policy`	Chybí	`strict-origin-when-cross-origin`

DOPORUČENÍ

Přidat hlavičky na úrovni nginx reverse proxy nebo ASP.NET middleware. Příklad pro nginx:

```
# /etc/nginx/conf.d/security-headers.conf
add_header Strict-Transport-Security "max-age=31536000; includeSubDomains" always;
add_header X-Content-Type-Options "nosniff" always;
add_header Referrer-Policy "strict-origin-when-cross-origin" always;
add_header Permissions-Policy "camera=(), microphone=(), geolocation=()" always;
```

10 • SOUHRN

Matice nálezů a pořadí *oprav.*

#	ZÁVAŽNOST	NÁLEZ	CWE	AKTIVUM	OPRAVA
F-01	KRITICKÝ	IDOR na payroll API — přístup k ~ 85 000 mzdovým záznamům	862	API	Okamžitě
F-02	VYSOKÝ	RCE přes Newtonsoft.Json deserializaci	502	API	Release
F-03	VYSOKÝ	Hardcoded Azure Storage master key v APK	798	APK	Do 7 dnů
F-04	STŘEDNÍ	Admin portál veřejně přístupný	749	Web	Release
F-05	STŘEDNÍ	Chybějící rate limiting na login	307	API	Release
F-06	INFO	Zastaralé knihovny (4×)	1104	API	Maintenance
F-07	INFO	Chybějící security headers (5×)	693	Web	Maintenance

Bezplatný opakovaný test

Součástí zakázky je bezplatný opakovaný test všech fakturovatelných nálezů (F-01 až F-05) do 60 dní od doručení této zprávy, maximálně tři testy na jeden nález. Po implementaci oprav nás kontaktujte a domluvíme termín opakovaného testu.

Omezení rozsahu a platnosti. Tato zpráva popisuje nálezy identifikované během penetračního testování v období 1.–7. dubna 2026 na aktivech definovaných v sekci 01. Testování je bodové ověření — odráží stav systémů v době provedení; pozdější změny mohou přinést nové zranitelnosti. Metodologie pokrývá nejčastější třídy zranitelností, ale není vyčerpávající; absence nálezu neznamená absenci zranitelnosti. Tato zpráva nepředstavuje certifikaci bezpečnosti. Doporučujeme pravidelné opakování testování minimálně každých 6 měsíců nebo po významných změnách systému.